UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/627,017	07/25/2003	John Mendonca	200209600-1	3688

22879 7590 01/11/2007

HEWLETT PACKARD COMPANY
P O BOX 272400, 3404 E. HARMONY ROAD
INTELLECTUAL PROPERTY ADMINISTRATION
FORT COLLINS, CO 80527-2400

EXAMINER	
OKORONKWO, CHINWENDU C	
ART UNIT	**PAPER NUMBER**
2136	

SHORTENED STATUTORY PERIOD OF RESPONSE	MAIL DATE	DELIVERY MODE
3 MONTHS	01/11/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

Office Action Summary	Application No.	Applicant(s)	
	10/627,017	MENDONCA ET AL.	
	Examiner	Art Unit	
	Chinwendu C. Okoronkwo	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *25 July 2003*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-20* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-20* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *25 July 2003* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. Pursuant to USC 131, claims 1-28 are presented for examination.

2. Claims 1-28 are pending.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

Claims 1-20 are rejected under 35 U.S.C. 102() as being disclosed by Shanklin et al. (U.S. Patent No. 6578147 B1).

Regarding claim 1, Shanklin et al., discloses a method of managing utilization of network intrusion detection systems in a dynamic data center, said method comprising: providing a plurality of network intrusion detection systems, each being networked so that utilization of each network intrusion detection system can be based on demand for said network intrusion detection systems in said dynamic data center; receiving a monitoring policy and a plurality of monitoring points to be monitored on a network with any of said network intrusion detection systems; and automatically arranging the monitoring of said monitoring points

using said network intrusion detection systems and said monitoring policy (col. 1 lines 63-67 and col. 2 lines 1-18).

Regarding claim 2, Shanklin et al., discloses the method as recited in claim 1 wherein said automatically arranging the monitoring of said monitoring points includes: automatically configuring a plurality of network resources to provide network communication data from said monitoring points to a plurality of available network intrusion detection systems from said network intrusion detection systems; and automatically configuring said available network intrusion detection systems to receive said network communication data based on said monitoring policy (col. 4 lines 43-67 and col. 5 lines 1-11).

Regarding claim 3, Shanklin et al., discloses the method as recited in claim 2 wherein said automatically arranging the monitoring of said monitoring points further includes: automatically increasing a number of particular network intrusion detection systems receiving said network communication data from a particular monitoring point by selecting additional available network intrusion detection systems if said network communication data exceeds a capacity of said particular network intrusion detection systems (col. 5 lines 14-67 and col. 6 lines 1-55).

Regarding claim 4, Shanklin et al., discloses the method as recited in claim 2 wherein said automatically arranging the monitoring of said monitoring points

further includes: automatically decreasing a number of particular network intrusion detection systems receiving said network communication data from a particular monitoring point by releasing any of said particular network intrusion detection systems to said available network intrusion detection systems if said network communication data is below a predetermined threshold of a capacity of said particular network intrusion detection systems (col. 5 lines 14-67 and col. 6 lines 1-55).

Regarding claim 5, Shanklin et al., discloses the method as recited in claim 2 wherein said network resources include one of a firewall, a gateway system, a network switch, and a network router (col. 6 lines 58-67 and col. 7 lines 1-38).

Regarding claim 6, Shanklin et al., discloses the method as recited in claim 1 wherein said receiving a monitoring policy and a plurality of monitoring points to be monitored includes: providing a graphical user interface to receive said monitoring policy and said plurality of monitoring points to be monitored (col. 3 lines 54-65).

Regarding claim 7, Shanklin et al., discloses the method as recited in claim 1 wherein said dynamic data center is a utility data center (col. 1 lines 63-67 and col. 2 lines 1-18).

Regarding claim 8, Shanklin et al., discloses a computer-readable medium comprising computer-executable instructions stored therein for performing a method of managing utilization of network intrusion detection systems in a dynamic data center, said method comprising: providing a plurality of network intrusion detection systems, each being networked so that utilization of each network intrusion detection system can be based on demand for said network intrusion detection systems in said dynamic data center; receiving a monitoring policy and a plurality of monitoring points to be monitored on a network with any of said network intrusion detection systems; and automatically arranging the monitoring of said monitoring points using said network intrusion detection systems and said monitoring policy (Rejected under the same rationale as claim 1).

Regarding claim 9, Shanklin et al., discloses the computer-readable medium as recited in claim 8 wherein said automatically arranging the monitoring of said monitoring points includes: automatically configuring a plurality of network resources to provide network communication data from said monitoring points to a plurality of available network intrusion detection systems from said network intrusion detection systems; and automatically configuring said available network intrusion detection systems to receive said network communication data based on said monitoring policy (Rejected under the same rationale as claim 2).

Regarding claim 10, Shanklin et al., discloses the computer-readable medium as recited in claim 9 wherein said automatically arranging the monitoring of said monitoring points further includes: automatically increasing a number of particular network intrusion detection systems receiving said network communication data from a particular monitoring point by selecting additional available network intrusion detection systems if said network communication data exceeds a capacity of said particular network intrusion detection systems (Rejected under the same rationale as claim 3).

Regarding claim 11, Shanklin et al., discloses the computer-readable medium as recited in claim 9 wherein said automatically arranging the monitoring of said monitoring points further includes: automatically decreasing a number of particular network intrusion detection systems receiving said network communication data from a particular monitoring point by releasing any of said particular network intrusion detection systems to said available network intrusion detection systems if said network communication data is below a predetermined threshold of a capacity of said particular network intrusion detection systems (Rejected under the same rationale as claim 4).

Regarding claim 12, Shanklin et al., discloses the computer-readable medium as recited in claim 9 wherein said network resources include one of a firewall, a

gateway system, a network switch, and a network router (Rejected under the same rationale as claim 5).

Regarding claim 13, Shanklin et al., discloses the computer-readable medium as recited in claim 8 wherein said receiving a monitoring policy and a plurality of monitoring points to be monitored includes: providing a graphical user interface to receive said monitoring policy and said plurality of monitoring points to be monitored (Rejected under the same rationale as claim 6).

Regarding claim 14, Shanklin et al., discloses the computer-readable medium as recited in claim 8 wherein said dynamic data center is a utility data center (Rejected under the same rationale as claim 7).

Regarding claim 15, Shanklin et al., discloses the system comprising: a dynamic data center including: a plurality of network resources; a plurality of network intrusion detection systems, each being networked so that utilization of each network intrusion detection system can be based on demand for said network intrusion detection systems in said dynamic data center; a graphical user interface for receiving a monitoring policy and a plurality of monitoring points to be monitored on a network with any of said network intrusion detection systems; and a controller for controlling said network resources and said network intrusion detection systems and for automatically arranging the monitoring of said

monitoring points using said network intrusion detection systems and said monitoring policy (Rejected under the same rationale as claim 1).

Regarding claim 16, Shanklin et al., discloses the system as recited in claim 15 wherein said controller automatically configures said network resources to provide network communication data from said monitoring points to a plurality of available network intrusion detection systems from said network intrusion detection systems, and wherein said controller automatically configures said available network intrusion detection systems to receive said network communication data based on said monitoring policy (Rejected under the same rationale as claim 2).

Regarding claim 17, Shanklin et al., discloses the system as recited in claim 16 wherein said controller automatically increases a number of particular network intrusion detection systems receiving said network communication data from a particular monitoring point by selecting additional available network intrusion detection systems if said network communication data exceeds a capacity of said particular network intrusion detection systems (Rejected under the same rationale as claim 3).

Regarding claim 18, Shanklin et al., discloses the system as recited in claim 16 wherein said controller automatically decreases a number of particular network

intrusion detection systems receiving said network communication data from a particular monitoring point by releasing any of said particular network intrusion detection systems to said available network intrusion detection systems if said network communication data is below a predetermined threshold of a capacity of said particular network intrusion detection systems (Rejected under the same rationale as claim 4).

Regarding claim 19, Shanklin et al., discloses the system as recited in claim 15 wherein said network resources include one of a firewall, a gateway system, a network switch, and a network router (Rejected under the same rationale as claim 5).

Regarding claim 20, Shanklin et al., discloses the system as recited in claim 15 wherein said dynamic data center is a utility data center (Rejected under the same rationale as claim 7).

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Chinwendu C. Okoronkwo whose telephone number is (571) 272 2662. The examiner can normally be reached on MWF 9:30 - 7:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nasser Moazzami can be reached on (571) 272 4195. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

CCO

January 6, 2007

NASSER MOAZZAMI
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

1/7/07